

In the Claims:

Please cancel claims 2 and 21-26. Please add new claims 27-33. The claims are as follows:

1. (Original) A method of forming a security enclosure, comprising:

providing an electronic assembly;

enclosing the assembly in a tamper respondent wrap, such that the wrap forms fold lines at a first and second end of the assembly;

placing the enclosed assembly in a fixture, wherein the fixture comprises a base upon which the assembly rests, a first stationary arm mounted on the base holding the fold lines at the first end of the assembly, a second arm slidably mounted on the base, and a traversing mechanism to bias the second arm toward the fold lines at the second end of the assembly; and

heating the enclosed assembly.

2. (Canceled)

3. (Previously presented) The method of claim 1, further comprising heating the enclosed assembly at a temperature of 40-90 °C.

4. (Previously presented) The method of claim 1, further comprising heating the enclosed assembly for 1 hour.

5. (Original) The method of claim 1, wherein the fixture comprises a clamping device.

09/654,543

2

6. (Original) The method of claim 1, wherein the tamper respondent wrap comprises a flexible material having tamper respondent detection devices.

7. (Original) The method of claim 1, wherein the tamper respondent wrap comprises:

at least one pierce and laser respondent layer;

a delamination respondent layer; and

an adhesive between the pierce and laser respondent layer and the delamination respondent layer.

8. (Original) The method of claim 7, wherein the pierce and laser respondent layer and the delamination respondent layer comprise a plurality of ink lines on at least one side of the pierce and laser respondent layer and the delamination respondent layer.

9. (Original) The method of claim 1, wherein the electronic assembly comprises a cryptographic processor.

10. (Original) The method of claim 9, wherein the cryptographic processor comprises a printed circuit board, having mounted thereon:

an encryption module to carry secured sensitive information;

a memory to store a key necessary to access the information;

an erase circuit to erase the information in the encryption module in the event the tamper respondent wrap is breached; and

an enclosure monitor to activate the erase circuit in the event a breach is detected.

11. (Original) A method of producing a tamper respondent enclosure, comprising:

enclosing a cryptographic processor in a tamper respondent sheet, wherein an adhesive material secures the enclosure;

holding the enclosed cryptographic processor such that the adhesive material remains intact; and

applying heat to the enclosed cryptographic processor to strengthen the adhesive material.

12. (Original) The method of claim 11, further including holding the enclosed cryptographic processor in a clamping device.

13. (Previously presented) The method of claim 11, further including applying heat at a temperature of 60 °C.

14. (Previously presented) The method of claim 11, further including applying heat at a temperature of 50-70 °C.

15. (Original) A method of forming a security enclosure, comprising:

providing a circuit card;

enclosing the card in a tamper respondent cloth, wherein an adhesive secures fold lines of the cloth;

holding the fold lines of the cloth to maintain adhesive contact; and

heating the enclosed card.

16. (Original) The method of claim 15, further comprising holding the cloth in a clamping device to maintain the adhesive contact.

17. (Original) The method of claim 16, wherein the clamping device comprises:

a base upon which a security enclosure rests;

a first stationary arm mounted on the base, which holds a first end of the security enclosure;

a second arm slidably mounted on the base; and

a traversing mechanism to bias the second arm toward a second end of the security enclosure.

18. (Previously presented) The method of claim 15, further comprising heating the enclosed card at 60 °C for 1 hour.

19. (Original) The method of claim 15, further comprising curing the adhesive.

20. (Original) The method of claim 15, wherein the circuit card comprises a cryptographic processor.

21-26. (Canceled)

27. (New) A security enclosure, comprising:

an electronic assembly;

a tamper respondent wrap, such that the wrap forms fold lines at a first and second end of the assembly, said wrap enclosing the electronic assembly; and

a fixture in which the enclosed assembly is placed, wherein the fixture comprises a base upon which the assembly rests, a first stationary arm mounted on the base holding the fold lines at the first end of the assembly, a second arm slidably mounted on the base, and a traversing mechanism to bias the second arm toward the fold lines at the second end of the assembly.

28. (New) The security enclosure of claim 27, wherein the fixture comprises a clamping device.

29. (New) The security enclosure of claim 27, wherein the tamper respondent wrap comprises a flexible material having tamper respondent detection devices.

30. (New) The security enclosure of claim 27, wherein the tamper respondent wrap comprises:

at least one pierce and laser respondent layer;

a delamination respondent layer; and

an adhesive between the pierce and laser respondent layer and the delamination respondent layer.

31. (New) The security enclosure of claim 30, wherein the pierce and laser respondent layer and the delamination respondent layer comprise a plurality of ink lines on at least one side of the pierce and laser respondent layer and the delamination respondent layer.

32. (New) The security enclosure of claim 27, wherein the electronic assembly comprises a cryptographic processor.

33. (New) The security enclosure of claim 32, wherein the cryptographic processor comprises a printed circuit board, having mounted thereon:

- an encryption module to carry secured sensitive information;

- a memory to store a key necessary to access the information;

- an erase circuit to erase the information in the encryption module in the event the tamper respondent wrap is breached; and

- an enclosure monitor to activate the erase circuit in the event a breach is detected.

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**